

REMARKS

This Amendment is filed together with a Request for Continued Examination (RCE) and the requisite RCE fee in response to the Examiner's Final Action dated June 16, 2008 and the Advisory Action dated October 3, 2008. Additionally, submitted herewith is a request for a 3 month extension of time together with the requisite extension fee for a large entity. Authorization is given to charge our Deposit Account 22-0261 with any additional fees that may be required by this submission.

Claims 1-6 were previously pending in the application. By this Amendment, claims 1, 4, 5 have been amended. Support for the amendments can be found on page 4 of the specification as originally filed. Claim 6 has been cancelled without prejudice or disclaimer. New claims 7, 8, 9, and 10 are added which parallel the content of the original claims. No new matter has been added. Accordingly, claims 1-5 and 7-10 are currently pending, with claims 1, 7 and 10 being independent claims.

It is respectfully submitted that the application in condition for allowance in view of the foregoing amendments and the following arguments.

Claim rejections under 35 USC § 102(e)

Claims 1, 4, 5 and 6 are rejected as being anticipated by US 6961857 (Floryanzia). It is respectfully submitted that claim 1 is substantially different and patentably distinguishable with respect to Floryanzia for the following reasons:

(1) Floryanzia in column 3 lines 58-61, Fig.3B, 4C and 4D discloses that an authentication server authenticates the information in the token and responds with either an Access-Accept or Access-Reject message. It should be clear that Floryanzia teaches that in the process of authentication, the authentication server performs both an encryption calculation and a determination of the legality of the gateway.

The Floryanzia authentication process is fundamentally different from the authentication method recited in claim 1 of the present application. Specifically, claim 1 recites, in part:

performing an encryption calculation according to the security authentication parameter and the authentication key and reporting a calculation result to the MGC, by the MG; and

determining by the MGC whether the MG is legal by comparing the calculation result with a result calculated by the MGC. (Emphasis added)

It is therefore clear that according to the presently claimed invention **the MG performs the encryption calculation and the MGC performs the determination of the legality of the MG**. Therefore, **contrary to the disclosure of Floryanzia, the two processes, namely encryption on the one hand and determining the legality on the other hand, are performed in two different devices**.

Further, in the authentication method of claim 1, the MGC, as a functional entity to authenticate the MG and determine the legality of access of the MG, initiates the authentication process by sending a security authentication request containing a security authentication parameter to the MG using the security data package; in Floryanzia, the authentication server is the functional entity to authenticate and determine the legality of the access, **but the initiator of the authentication process in Floryanzia is the gateway** (See column 3 lines 58-61, Fig.3A, 3B). Claim 1, on the other hand, recites “during a security authentication, **sending by the MGC a security authentication request containing a security authentication parameter to the MG using the data package....**” This is therefore a further distinguishing feature between claim 1 and Floryanzia because in Floryanzia the authentication process is initiated in the gateway. As described on page 3, lines 6-14 of the present application, because of this distinguishing feature, the authentication of the MG can be controlled by the MGC whenever the MGC considers authentication to be necessary, thus providing a “kind of authentication [that] has a characteristic of randomness and higher security authentication efficiency.”

Because the authentication of the MG is under the control of the MGC, the data used for the authentication is set by the MGC (including the authentication key, the security data package and the security authentication request). By contrast, in Floryanzia, the access party or gateway is the initiator of the authentication process, and provides most data used for authentication (e.g. Token). The authentication method recited by claim 1 has higher security and efficiency than Floryanzia.

For the foregoing reasons, Applicants respectfully submit that the invention recited by claim 1 is not anticipated by Floryanzia. Claims 4 and 5 depend from and incorporate the limitations of claim 1, and are submitted to be patentable for at least the same reasons as advanced above in connection with claim 1. As previously noted, claim 6 is cancelled herein without prejudice.

Claim 4 is submitted to be patentable for the further reason that Floryanzia does not disclose “said data package comprises a security authentication request signal and a security authentication completion event, said security authentication request signal comprises a security authentication parameter, and said security authentication completion event comprises a security authentication result parameter; the step of reporting a calculation result includes reporting by the calculation result to the MGC via a security authentication completion event in a data package.” By using the authentication method of claim 4, the MGC as the functional entity to authenticate and determine the legality of the access can control the reporting process of the MG as the access party, and this can also improve the security and efficiency of the authentication process. In another aspect, setting a security authentication completion event to control the reporting is easy for the MG to implement as an event can be simply identified by the MG. So, the invention as further recited by claim 4 reduces the complexity of the MG and the interaction between the MGC and the MG.

Claim rejections under 35 USC § 103

Claims 2 and 3 stand rejected under 35 USC § 103 as being unpatentable over Floryanzia in view of US20020120760 (Kimchi). It is requested that this rejection be reconsidered and withdrawn for the principal reason that dependent claims 2 and 3 include the technical features of claim 1 and Kimchi fails to cure the deficiencies of Floryanzia as discussed above with respect to claim 1. Therefore, it is submitted that claims 2 and 3 are patentable over any reasonable combination of Floryanzia and Kimchi.

New claims 7-10

New claims 7-10 include the technical features of claims 1, 4 and 5 that distinguish these latter claims over the prior art, including Floryanzia and Kimchi, as discussed above. Additionally, neither Floryanzia nor Kimchi, teach or otherwise disclose the following feature in new claims 7-10: “applicable in a Next Generation Network (NGN).” This feature is supported by the disclosure on page 1, lines 8-13 and page 2, lines 3-4 of the specification as originally filed. Claims 7-10 are therefore submitted to be novel and non-obvious over any reasonable reading of Floryanzia and Kimchi.

Conclusion

Pending claims 1-5 and 7-10 are submitted to be in condition for allowance, and Applicant respectfully requests issuance of the subject application. If any issues remain that preclude issuance of the application, the Examiner is invited to contact the undersigned attorney before issuing a subsequent Action.

Dated: December 15, 2008

Respectfully submitted,

By /Robert Kinberg/
Robert Kinberg
Registration No.: 26,924
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
202-344-4000
202-344-8400 (Fax)
Attorney/Agent For Applicant

RK/aaw

#1003430